

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF NORTH CAROLINA
CHARLOTTE DIVISION

MAR 12 2019

US DISTRICT COURT
WESTERN DISTRICT OF NC

UNITED STATES OF AMERICA

DOCKET NO. **3:19-cr-78-MOC**

v.

BILL OF INFORMATION

Violations: 18 U.S.C. § 371

BISHAP MITTAL

THE UNITED STATES ATTORNEY CHARGES:

At the specified times and at all relevant times:

1. Defendant Bishop Mittal knowingly participated in an international conspiracy to place malicious pop-ups on victims' computers, inducing them to call the conspirators' technical support front companies to purchase purported "technical support" services. The conspiracy caused more than \$3,000,000.00 in actual damages to hundreds of victims throughout the United States.

Background

2. Capstone Technologies LLC was a company headquartered in Charlotte, North Carolina, within the Western District of North Carolina, that claimed to provide computer-related services to its customers. Capstone Technologies LLC conducted business using several different aliases, including—but not limited to—Authenza Solutions LLC, MS-Squad Technologies, MS-Squad.com, MS Infotech, United Technologies, and Reventus Technologies, (collectively "Capstone Technologies.")

3. Individual 1, was the owner and/or manager of Capstone Technologies. Individual 1 resided in the Western District of North Carolina.

4. Bishop Mittal ("BISHAP") incorporated United Technologies. BISHAP resided with Individual 1 in the Western District of North Carolina.

5. Microsoft Corporation is an internet service provider and software company whose normal activities took place in interstate and foreign commerce, and had an effect on interstate and foreign commerce. Bing is an internet search engine that is owned and operated by Microsoft. Microsoft's online advertising platform is known as Bing Ads.

6. Google LLC is an internet service provider and software company whose normal activities took place in interstate and foreign commerce, and had an effect on interstate and foreign commerce. Google is an internet search engine that is owned and operated by Google LLC. Google LLC's online advertising platform is known as Google Ads.

7. Throughout this Information, the word “pop-up” refers to a form of adware that temporarily locks victims’ computers and displays a message directing victims to contact a toll-free number of technical assistance to remove the pop-up. Pop-ups often include inflammatory and/or misleading representations of diagnosing systemic network infirmities, including viruses and instances of hacking, all in an effort to delude victims into seeking technical assistance.

8. A call center is an office that is established to manage and handle a large volume of telephone calls in the course of taking orders and providing customer assistance.

9. Search Engine Optimization (“SEO”) is the process of maximizing the number of visitors to a particular website by ensuring that the company’s site appears prominently on the list of results returned by internet search engines like Bing and Google.

The Technical Support (“Tech-Support”) Scheme

10. Individual 1, BISHAP, and others known and unknown to the United States Attorney created Capstone Technologies, established financial accounts for those entities, and then used a call center located in the New Delhi area of the Republic of India to handle incoming and outgoing interactions with potential victims. The call center conspirators offered purported tech-support services to victims and connected to victims’ computers using remote access tools.

11. After remotely connecting to victims’ computers, the call center conspirators often falsely stated that routine computer functions and processes were evidence of problems with the computer. In addition, the call center conspirators often falsely stated that the consumers’ computers were infected with viruses or malware.

12. A script for the call center employees encouraged them to misleadingly tell victims who had two antivirus applications that the two applications were “contradicting each other.” The script also suggested that the employees misleadingly tell victims that the identification of foreign addresses “may to [sic] show computer compromising.” Furthermore, the script told employees to use Command Prompt tools to generate outputs that would purportedly indicate a “virus found or network infection.”

13. Individual 1, BISHAP, and others known and unknown to the United States Attorney used multiple strategies to reach potential victims, including SEO, advertisement space on Google Ads and Bing ads, and malicious pop-ups. Regardless of the method of contact, India-based technicians misrepresented various computer infirmities to delude victims into purchasing unnecessary tech-support services. The victims’ purchases ranged from approximately \$200 to more than \$2,400.

14. Pop-ups were a central part of the scheme. Individual 1 and others known and unknown to the United States Attorney purchased blocks of malicious pop-ups from publishers around the world. When the pop-ups appeared on victims’ computers, they would render the machine temporarily inoperable under the guise of detecting a supposed systemic computer failure. Some of these pop-ups misrepresented that the computer failures had been identified and diagnosed by Microsoft Corporation—a misrepresentation that company technicians reiterated during direct interactions with victims. Regardless of the content of specific pop-ups, each version had the same

function: to induce unsuspecting computer users into contacting a representative of Capstone Technologies for the performance of unnecessary tech-support services.

Count One

(18 U.S.C. § 371 – Conspiracy to Access A Protected Computer)

15. The United States Attorney incorporates the allegations in paragraphs One through Fourteen of this Bill of Information.

16. From no earlier than November 2014 until not later than August 2018, in the Western District of North Carolina and elsewhere, the defendant:

BISHAP MITTAL

knowingly conspired and agreed, with other persons known and unknown to the United States Attorney, to intentionally accessed a protected computer without authorization, and as a result of such conduct, caused damage, in violation of 18 U.S.C. §§ 1030(a)(5)(C) and (c)(4)(G).

Object of the Conspiracy

17. It was a part of and an object of the conspiracy that the defendant and others known and unknown to the United States Attorney intentionally accessed a protected computer without authorization, and as a result of such conduct, caused damage, in violation of 18 U.S.C. §§ 1030(a)(5)(C) and (c)(4)(G).

Manner and Means

18. The defendant and others known and unknown to the United States Attorney carried out the conspiracy through the manner and means described in paragraphs One through Fourteen of this Bill of Information, among others.

Overt Acts

19. To accomplish the object of the conspiracy, the defendant and his co-conspirators committed the following acts, among others, in furtherance of their unlawful goals:

- a. On or about December 19, 2015, a call center conspirator remotely accessed the computer of a victim who had called in response to a malicious pop-up on her computer and made misleading claims in an attempt to persuade her to purchase tech support services;
- b. On or about February 8, 2016, BISHAP incorporated one of the Capstone Technologies companies; and
- c. On or about July 26, 2016, BISHAP communicated with Individual 1 regarding the misuse of a publicly available remote access tool by Capstone Technologies conspirators, including the use of malicious pop-up ads that blocked victims' screens until they called Capstone Technologies.

All in violation of 18 U.S.C. 371.

NOTICE OF FORFEITURE AND FINDING OF PROBABLE CAUSE

Notice is hereby given of 18 U.S.C. § 982 and 28 U.S.C. § 2461(c). Under Section 2461(c), criminal forfeiture is applicable to any offenses for which forfeiture is authorized by any other statute, including but not limited to 18 U.S.C. § 981 and all specified unlawful activities listed or referenced in 18 U.S.C. § 1956(c)(7), which are incorporated as to proceeds by § 981(a)(1)(C). The following property is subject to forfeiture in accordance with §§ 982 and/or 2461(c):

- a. All property which constitutes or is derived from proceeds of the violations set forth in this Bill of Information; and
- b. If, as set forth in 21 U.S.C. § 853(p), any property described in (a) cannot be located upon the exercise of due diligence, has been transferred or sold to, or deposited with, a third party, has been placed beyond the jurisdiction of the court, has been substantially diminished in value, or has been commingled with other property which cannot be divided without difficulty, all other property of the defendant/s to the extent of the value of the property described in (a).

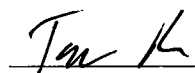
There is probable cause to believe that the following property is subject to forfeiture on one or more of the grounds stated above:

- a. A forfeiture money judgment in the amount of at least \$150,000, such amount constituting the proceeds of the violations set forth in this Bill of Information.

WILLIAM STETZER
ATTORNEY FOR THE UNITED STATES¹

 (by TSP)

TIMOTHY C. FLOWERS
SENIOR TRIAL ATTORNEY
COMPUTER CRIME & INTELLECTUAL PROPERTY SECTION



TAYLOR J. PHILLIPS
ASSISTANT UNITED STATES ATTORNEY

¹ Acting under authority conferred by 28 U.S.C. § 515.